IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

FIRST NAMED INVENTOR	:	Nancy Cam WINGET	**Confirmation No.: 3154**
FOR	:	SYSTEM AND METHOD FOR PROVISIONING AND AUTHENTICATING VIA A NETWORK	
APPLICATION NO.	:	10/724,995	
FILING DATE	:	December 1, 2003	
EXAMINER	:	Jeffrey D. Popham	
ART UNIT	:	2437	
CUSTOMER NO.	**:**	**23380**	

APPEAL BRIEF

Mail Stop Appeal Briefs - Patent
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

The Final Office Action in the above-identified application was dated April 10, 2009. Applicant filed a Notice of Appeal on July 10, 2009.

Favorable consideration of the instant Appeal Brief is respectfully requested.

TABLE OF CONTENTS

REAL PARTY IN INTEREST

This application has been assigned to Cisco Technology, Inc. having a place of business at 170 W. Tasman Drive San Jose, California 95134. Cisco Technology, Inc. is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no related appeals and interferences to this Appeal.

STATUS OF CLAIMS

Claims 1, 2, 5-10, 15-21, 24, 26, and 27 are pending and under final rejection. Claims 3-4, 11-14, 22-23, and 25 have been canceled. Claims 1, 2, 5-10, 15-21, 24, 26, and 27 are on appeal.

STATUS OF AMENDMENTS

An amendment was filed on June 25, 2009 and has been entered by the Examiner.

SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 recites a method of authenticating communication between a first and a second party (page 7, lines 13-14). The method includes determining whether a shared secret exists between a peer and a server (page 29, line 4). The method includes establishing a first secure tunnel between the peer and the server using asymmetric encryption responsive to determining the shared secret does not exist between the peer and the server (page 27, line 15 – page 28, line 4). The method includes receiving the shared secret via the first secure tunnel between the peer and the server responsive to determining that the shared secret does not exists between the peer and the server and to establishing the first secure tunnel (page 28, lines 22-24). The method includes tearing down the first secure tunnel (page 28, line 25-page 29, line 1). The method includes establishing a subsequent new secure tunnel between the peer and the server using symmetric encryption and the shared secret after the tearing down the first secure tunnel and after the peer has received the shared secret (page 29, lines 3-11). The method includes mutually deriving a tunnel key for the subsequent new secure tunnel using symmetric cryptography based on the shared secret responsive to establishing the subsequent new secure tunnel (page 29, lines 12-16). The method includes authenticating a relationship between the peer and the server within the subsequent new secure tunnel upon mutually deriving the tunnel key for the subsequent new secure tunnel (page 29, lines 21-25). The method includes cryptographically binding the subsequent new secure tunnel with conversations inside the subsequent new secure tunnel (page 29, line 26-page 30, line 2).

Independent claim 17 recites a system for communicating via a network (page 14, lines 7-10). The system comprises means for providing a communication link between a peer and a server (Provisioning Phase 130, Tunnel Establishment Phase 140, and Authentication Phase 150, Fig. 1). The system comprises means for determining whether a shared secret exists between the peer and the server (EAP-Fast Server 220, Fig. 2 and page 29, line 4). The system comprises means for provisioning a shared secret between the peer and the server responsive to means for determining whether the shared secret exists determining the shared secret does not exist (EAP-Fast Server 220, Fig. 2). The means for provisioning comprises means for establishing a first secure tunnel between the peer server using asymmetric encryption (EAP-Fast Server 220, Fig. 2 and page 27, line 15 – page 28, line 4). The means for provisioning comprises means for acquiring the shared secret through the first tunnel (EAP-Fast Server 220, Fig. 2 and page 28, lines 22-24). The mans for provisioning comprises means for tearing down the first secure tunnel after the means for acquiring has acquired the shared secret (EAP-Fast Server 220, Fig. 2 and page 28, line 25-page 29, line 1). The system comprises means for establishing a subsequent new secure tunnel utilizing the shared secret after the means for tearing down has torn down the first secure tunnel and responsive to the means for determining whether a shared secret exists determining that the shared secret exists (EAP-Fast Server 220, Fig. 2 and page 29, lines 3-11). The means for establishing subsequent new secure tunnel comprises means for deriving a tunnel key using symmetric cryptography based on the shared secret (page 29, lines 12-16). The system comprises means for authenticating a relationship between the peer and the server within the subsequent new secure tunnel (Authenticator 230, Fig. 2 and page 29, lines 21-25). The system comprises means for cryptographically binding the subsequent new secure tunnel with conversations inside the subsequent new secure tunnel (EAP-Fast Server 220, Fig. 2 and page 29, line 26-page 30, line 2).

Independent claim 24 recites a wireless device comprising a wireless network adapter for sending and receiving wireless signals with a server (page 17, lines 7-9). The wireless device is configured to determine whether a shared secret exists between the wireless device and the server (page 29, line 4). The wireless device is configured to receive a shared secret from the server upon determining that a shared secret does exist with the server (page 15, lines 17-20 and page 27, line 15 – page 28, line 4). The shared secret is received by establishing a first secure tunnel with a server using asymmetric encryption, receiving the shared secret via the first secure tunnel from the server, and tearing down the first secure tunnel after receiving the shared secret (page 28, line 22 - page 29, line 1). The wireless device is configured to establish a subsequent new secure tunnel between the wireless device and the server after the first secure tunnel has been torn down and upon determining the shared secret exists by using the shared secret to mutually derive a tunnel key using symmetric cryptography based on the shared secret (page 16, lines 15-17 and page 29, lines 3-11). The wireless device is configured to mutually authenticate with the server employing the subsequent new secure tunnel (page 16, lines 15-17). The wireless device is configured to derive keying material that binds the subsequent new secure tunnel with all conversations inside the subsequent new secure tunnel (page 16, lines 17-20).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

I. Whether claims 1-2, 5-6 9-10 15-21, 24, and 26-27 are obvious under U.S.C. § 103(a) in view of the combination of U.S. Patent Application Publication 2004/0268126 to Dogan et al. (*hereinafter* Dogan), U.S. Patent 6,978,298 to Kuehr-McLaren (*hereinafter* Kuehr-McLaren), and Paul Funk, Somin Blak Wilson, "drat-ietf-eap-ttls-02.txt: EAP Tunneled TLS Authentication Protocol (EAO-TTLS)"; Internet draft PPPEXT Working Group; 30 Nov. 2002, pp. 1-40 (*hereinafter* Funk).

ARGUMENT

Rejections under 35 U.S.C. § 103(a) over U.S. Patent Publication No. 2004/0268126, U.S. Patent No. 6,978,298, and EAP Tunneled TLS Authentication Protocol, Paul Funk and Somin Blak Wilson.

Claims 1-2, 5-6 9-10 15-21, 24, and 26-27 stand rejected under U.S.C. § 103(a) as being obvious in view of the combination of U.S. Patent Application Publication 2004/0268126 to Dogan et al. (*hereinafter* Dogan), U.S. Patent 6,978,298 to Kuehr-McLaren (*hereinafter* Kuehr-McLaren), and Paul Funk, Somin Blak Wilson, "draft-ietf-eap-ttls-02.txt: EAP Tunneled TLS Authentication Protocol (EAO-TTLS)"; Internet draft PPPEXT Working Group; 30 Nov. 2002, pp. 1-40 (*hereinafter* Funk). For the reasons that will now be set forth, claims 1-2, 5-6 9-10 15-21, 24, and 26-27 are not obvious in view of the combination of Dogan, Kuehr-McLaren, and Funk.

To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). *In re Vaeck*, 947 F.2d 488; 20 USPQ2d 1438 (Fed. Cir. 1991). "All words in a claim must be considered in judging the patentability of that claim against the prior art."

A. Claims 1-2, 5-10, 15-16, and 27

By way of review, independent claim 1 recites a method for authenticating communication between a first and second party via a network. A first secure tunnel is established between a peer and a server using asymmetric encryption in response to determining that a shared secret does not exist between the peer and the server. The shared secret is received via the first secure tunnel between the peer and the server and the first secure tunnel is then torn down. A subsequent new secure tunnel is established between the peer and the server using symmetric encryption and the shared secret after tearing down the first secure tunnel and after the peer has received the shared secret. A tunnel key is mutually derived for the subsequent new secure tunnel using symmetric cryptography based on the shared secret in response to establishing the subsequent new secure tunnel. A relationship between the peer and the server is then authenticated within the subsequent secure tunnel. The subsequent new secure tunnel is then cryptographically bound with conversations inside the subsequent new secure tunnel.

By contrast, Dogan teaches shared secret generation for symmetric cryptography. A master secret is established between a first communication device and a second communication device (see ¶7). A connection is opened between the first communication device and the second communication device (see ¶7). A connection secret is generated from the master secret and used as symmetric key during the life of the connection (see ¶7). To the contrary, Dogan teaches establishing the master secret during registration (see ¶23). The registration process is defined to include authentication of a user terminal (see ¶22). Thus, Dogan teaches both establishing a master secret and authenticating the peer using the first secure tunnel. A second tunnel is later opened when a user terminal indicates it needs to send data (¶24). Dogan does not teach or suggest cryptographically binding a subsequent secure tunnel with conversations inside the subsequent secure tunnel as recited in claim 1. This means that the conversation is associated with, or tied to, the tunnel. Cryptographically binding of the tunnel with the conversation inside the tunnel helps detect and prevent man-in-the-middle attacks which enable an adversary to take control of information between a peer and a server by impersonating the peer of the server. Dogan does not address the detection or prevention of such attacks. The Examiner argues that the entities of Dogan communicating inside the subsequent new secure tunnel by using the connection secret is the same as the conversation being bound to the tunnel. However, this does not detect or prevent man-in-the-middle attacks since a man-in-the-middle may impersonate a peer and begin communicating inside the tunnel. Unless the conversation between the peer and the server is bound to the tunnel, the communication between the peer and server is open to man-in-the-middle attacks. Thus, Dogan does not teach or suggest every element of independent claim 1.

The aforementioned deficiencies in Dogan are not remedied by any teachings of Kuehr-McLaren. Kuehr-McLaren teaches a method and apparatus for managing session information in a data processing system (Abstract). A request for a secure connection is received (Abstract). The secure connection is established, wherein information used to facilitate the secure connection is generated (Abstract). The information is stored for a selected period of time, wherein the selected period of time is selected to optimize server resources (Abstract). Kuehr-

McLaren, however, does not teach or suggest cryptographically binding a subsequent secure tunnel with conversations inside the tunnel. Kuehr-McLaren is relied on by the Examiner to teach determining whether a shared secret exists between a peer and a server.

The aforementioned deficiencies of Dogan and Kuehr-McLaren are not remedied by the teachings of Funk. Funk teaches using asymmetric encryption for establishing a tunnel and authenticating within the tunnel. Funk, however, does not teach or suggest cryptographically binding a subsequent secure tunnel with conversations inside the tunnel. As discussed herein, communicating within a secure tunnel does not detect or prevent man-in-the-middle attacks. Claim 1 remedies this problem by cryptographically binding the conversation within the tunnel the tunnel.

Therefore, for the reasons set forth; neither Dogan, McLaren or Funk, alone or in combination, teach or suggest all of the elements of independent claim 1. Thus, independent claim 1 is not obvious in view of Dogan, McLaren or Funk.

Claims 2, 5-10, 15-16, and 27 depend directly from claim 1 and therefore contain each and every element of claim 1. If an independent claim is nonobvious under 35 U.S.S. § 103, then any claim depending therefrom is nonobvious. *In re Fine,* 837 F.2d 1071, 5 USPQ2d 1956 (Fed. Cir. 1988). Thus, claims 2, 5-10, 15-16 and 27 are not obvious in view of Dogan, McLaren or Funk for the reasons already set forth for claim 1.

B. Claims 17-21

By way of review, independent claim 17 recites a system for communicating via a network. A first secure tunnel is established between a peer and a server using asymmetric encryption in response to determining that a shared secret does not exist between the peer and the server. The shared secret is received via the first secure tunnel between the peer and the server and the first secure tunnel is then torn down. A subsequent new secure tunnel is established between the peer and the server using symmetric encryption and the shared secret after tearing down the first secure tunnel and after the peer has received the shared secret. A tunnel key is mutually derived for the subsequent new secure tunnel using symmetric cryptography based on the shared secret in response to establishing the subsequent new secure tunnel. A relationship between the peer and the server is then authenticated within the subsequent secure tunnel. The subsequent new secure tunnel is then cryptographically bound with conversations inside the subsequent new secure tunnel.

By contrast, Dogan teaches shared secret generation for symmetric cryptography. A master secret is established between a first communication device and a second communication device (see ¶7). A connection is opened between the first communication device and the second communication device (see ¶7). A connection secret is generated from the master secret and used as symmetric key during the life of the connection (see ¶7). To the contrary, Dogan teaches establishing the master secret during registration (see ¶23). The registration process is defined to include authentication of a user terminal (see ¶22). Thus, Dogan teaches both establishing a master secret and authenticating the peer using the first secure tunnel. A second tunnel is later opened when a user terminal indicates it needs to send data (¶24). Dogan does not teach or suggest cryptographically binding a subsequent secure tunnel with conversations inside the tunnel as recited in claim 17. This means that the conversation is associated with, or tied to, the tunnel. Cryptographically binding of the tunnel with the conversation inside the tunnel helps detect and prevent man-in-the-middle attacks which enable an adversary to take control of information between a peer and a server by impersonating the peer of the server. Dogan does not address the detection or prevention of such attacks. The Examiner argues that the entities of Dogan communicating inside the subsequent new secure tunnel by using the connection secret is the same as the conversation being bound to the tunnel. However, this does not detect or prevent man-in-the-middle attacks since a man-in-the-middle may impersonate a peer and begin communicating inside the tunnel. Unless the conversation between the peer and the server is bound to the tunnel, the communication between the peer and server is open to man-in-the-middle attacks. Thus, Dogan does not teach or suggest every element of independent claim 17.

The aforementioned deficiencies in Dogan are not remedied by any teachings of Kuehr-McLaren. Kuehr-McLaren teaches a method and apparatus for managing session information in a data processing system (Abstract). A request for a secure connection is received (Abstract). The secure connection is established, wherein information used to facilitate the secure connection is generated (Abstract). The information is stored for a selected period of time, wherein the selected period of time is selected to optimize server resources (Abstract). Kuehr-McLaren, however, does not teach or suggest cryptographically binding a subsequent secure tunnel with conversations inside the tunnel. Kuehr-McLaren is relied on by the Examiner to teach determining whether a shared secret exists between a peer and a server.

The aforementioned deficiencies of Dogan and Kuehr-McLaren are not remedied by the teachings of Funk. Funk teaches using asymmetric encryption for establishing a tunnel and authenticating within the tunnel. Funk, like Dogan and Kuehr-McLaren, does not teach or suggest cryptographically binding a subsequent secure tunnel with conversations inside the tunnel. As discussed herein, communicating within a secure tunnel by itself does not detect or prevent man-in-the-middle. Claim 17 solves this problem by cryptographically binding conversation(s) within the tunnel to the tunnel.

Therefore, for the reasons set forth, neither Dogan, McLaren or Funk, alone or in combination, teach or suggest all of the elements of independent claim 17. Thus, independent claim 17 is not obvious in view of Dogan, McLaren or Funk.

Claims 18-21 depend directly from claim 17 and therefore contain each and every element of claim 17. If an independent claim is nonobvious under 35 U.S.S. § 103, then any claim depending therefrom is nonobvious. *In re Fine,* 837 F.2d 1071, 5 USPQ2d 1956 (Fed. Cir. 1988). Thus, claims 18-21 are not obvious in view of Dogan, McLaren or Funk for the reasons already set forth for claim 17.

C. Claims 24 and 26

By way of review, independent claim 24 recites a wireless device comprising a wireless network adapter for sending and receiving wireless signals with a server. The wireless device establishes a first secure tunnel between a peer and a server using asymmetric encryption in response to determining that a shared secret does not exist between the peer and the server. The wireless device receives the shared secret via the first secure tunnel between the peer and the server and the first secure tunnel is then torn down. The wireless device establishes a subsequent new secure tunnel between the peer and the server using symmetric encryption and the shared secret after tearing down the first secure tunnel and after the peer has received the shared secret. A tunnel key is mutually derived for the subsequent new secure tunnel using symmetric cryptography based on the shared secret in response to establishing the subsequent new secure tunnel. A relationship between the peer and the server is then authenticated within the subsequent secure tunnel. The wireless device derives keying material that binds the subsequent new secure tunnel with all conversations inside the subsequent new secure tunnel.

By contrast, Dogan teaches shared secret generation for symmetric cryptography. A master secret is established between a first communication device and a second communication device (see ¶7). A connection is opened between the first communication device and the second communication device (see ¶7). A connection secret is generated from the master secret and used as symmetric key during the life of the connection (see ¶7). To the contrary, Dogan teaches establishing the master secret during registration (see ¶23). The registration process is defined to include authentication of a user terminal (see ¶22). Thus, Dogan teaches both establishing a master secret and authenticating the peer using the first secure tunnel. A second tunnel is later opened when a user terminal indicates it needs to send data (¶24). Dogan does not teach or suggest binding a subsequent secure tunnel with conversations inside the tunnel as recited in claim 24. This means that the conversation is associated with, or tied to, the tunnel. Binding of the tunnel with the conversation inside the tunnel helps detect and prevent man-in-the-middle attacks which enable an adversary to take control of information between a peer and a server by impersonating the peer of the server. Dogan does not address the detection or prevention of such attacks. The Examiner argues that the entities of Dogan communicating inside the subsequent new secure tunnel by using the connection secret is the same as the conversation being bound to the tunnel. However, this does not detect or prevent man-in-the-middle attacks since a man-in-the-middle may impersonate a peer and begin communicating inside the tunnel. Unless the conversation between the peer and the server is bound to the tunnel, the communication between the peer and server is open to man-in-the-middle attacks. Thus, Dogan does not teach or suggest every element of independent claim 24.

The aforementioned deficiencies in Dogan are not remedied by any teachings of Kuehr-McLaren. Kuehr-McLaren teaches a method and apparatus for managing session information in a data processing system (Abstract). A request for a secure connection is received (Abstract). The secure connection is established, wherein information used to facilitate the secure connection is generated (Abstract). The information is stored for a selected period of time, wherein the selected period of time is selected to optimize server resources (Abstract). Kuehr-McLaren, however, does not teach or suggest cryptographically binding a subsequent secure tunnel with conversations inside the tunnel. Kuehr-McLaren is relied on by the Examiner to teach determining whether a shared secret exists between a peer and a server.

The aforementioned deficiencies of Dogan and Kuehr-McLaren are not remedied by the teachings of Funk. Funk teaches using asymmetric encryption for establishing a tunnel and authenticating within the tunnel. Funk, however, does not teach or suggest derives keying material that binds the subsequent new secure tunnel with all conversations inside the subsequent new secure tunnel. As discussed herein, communicating within a secure tunnel does not detect or prevent man-in-the-middle attacks. The device in claim 24 solves this by deriving keying material that binds the subsequent new secure tunnel with all conversations inside the subsequent new secure tunnel.

Therefore, for the reasons set forth, neither Dogan, McLaren or Funk, alone or in combination, teach or suggest all of the elements of independent claim 24. Thus, independent claim 24 is not obvious in view of Dogan, McLaren or Funk.

Claim 26 depends directly from claim 24 and therefore contains each and every element of claim 24. If an independent claim is nonobvious under 35 U.S.S. § 103, then any claim depending therefrom is nonobvious. *In re Fine,* 837 F.2d 1071, 5 USPQ2d 1956 (Fed. Cir. 1988). Thus, claim 26 is not obvious in view of Dogan, McLaren or Funk for the reasons already set forth for claim 24.

Conclusion

Withdrawal of the rejections to this application is requested for the reasons set forth herein and a Notice of Allowance is earnestly solicited. If there are any fees necessitated by the foregoing communication, the Commissioner is hereby authorized to charge such fees to our Deposit Account No. 50-0902, referencing our Docket No. 72255/:.00010

Respectfully submitted,

TUCKER ELLIS & WEST LLP

Date: September 4, 2009

By : Larry B. Donovan

Larry B. Donovan
Registration No. 47,230
Tucker Ellis & West LLP
1150 Huntington Building
925 Euclid Avenue
Cleveland, Ohio 44115-1475
Customer No. 23380
(phone) (216) 696-3864

CLAIMS APPENDIX

1. A method of authenticating communication between a first and a second party, the method comprising:

determining whether a shared secret exists between a peer and a server;

establishing a first secure tunnel between the peer and the server using asymmetric encryption responsive to determining the shared secret does not exist between the peer and the server;

receiving the shared secret via the first secure tunnel between the peer and the server responsive to the determining that the shared secret does not exist between the peer and the server and to the establishing the first secure tunnel;

tearing down the first secure tunnel;

establishing a subsequent new secure tunnel between the peer and the server using symmetric encryption and the shared secret after the tearing down the first secure tunnel and after the peer has received the shared secret;

mutually deriving a tunnel key for the subsequent new secure tunnel using symmetric cryptography based on the shared secret responsive to establishing the subsequent new secure tunnel;

authenticating a relationship between the peer and the server within the subsequent new secure tunnel upon mutually deriving the tunnel key for the subsequent new secure tunnel; and

cryptographically binding the subsequent new secure tunnel with conversations inside the subsequent new secure tunnel.

2. The method set forth in claim 1 further comprising the step of protecting the termination of the authenticated conversation by use of a tunnel encryption and authentication to protect against a denial of service by an unauthorized user.

5. The method set forth in claim 1 wherein the shared secret is a protected access credential (PAC).

6. The method set forth in claim 5 wherein the protected access credential includes a protected access credential key.

7. The method set forth in claim 6 wherein the protected access credential key is a strong entropy key.

8. The method set forth in claim 7 wherein the entropy key is a 32-octet key.

9. The method set forth in claim 6 wherein the protected access credential includes a protected access credential opaque element.

10. The method set forth in claim 6 wherein the protected access credential includes a protected access credential information element.

15. The method set forth in claim 1 wherein the step of authenticating is performed using EAP-GTC.

16. The method set forth in claim 1 wherein the step of authenticating is performed using Microsoft MS-CHAP v2.

17. A system for communicating via a network, the system comprising:

means for providing a communication link between a peer and a server;

means for determining whether a shared secret exists between the peer and the server;

means for provisioning a shared secret between the peer and the server responsive to the means for determining whether the shared secret exists determining the shared secret does not exist, wherein the means for provisioning comprises means for establishing a first secure tunnel between the peer and server using asymmetric encryption, means for acquiring the shared secret through the first secure tunnel, and means for tearing down the first secure tunnel after the means for acquiring has acquired the shared secret;

means for establishing a subsequent new secure tunnel utilizing the shared secret after the means for tearing down has torn down the first secure tunnel and responsive to the means for determining whether a shared secret exists determining that the shared secret exists, wherein the means for establishing the subsequent new secure tunnel comprises means for deriving a tunnel key using symmetric cryptography based on the shared secret;

means for authenticating a relationship between the peer and the server within the subsequent new secure tunnel; and

means for cryptographically binding the subsequent new secure tunnel with conversations inside the subsequent new secure tunnel.

18. The system for communicating set forth in claim 17 wherein the communication link is a wireless network.

19. The system for communicating set forth in claim 17 wherein the communication link is a wired network.

20. The system for communicating set forth in claim 17 wherein the shared secret is a protected access credential (PAC).

21. The system for communicating set forth in claim 18 wherein the wireless network is an 802.11 wireless network.

24. A wireless device, comprising:

a wireless network adapter for sending and receiving wireless signals with a server;

wherein the wireless device is configured to determine whether a shared secret exists between the wireless device and the server;

wherein the wireless device is configured to receive a shared secret from the server upon determining that a shared secret does not exist with the server, by establishing a first secure tunnel with server using asymmetric encryption, receiving the shared secret via the first secure tunnel from the server, and tearing down the first secure tunnel after receiving the shared secret;

wherein the wireless device is configured to establish a subsequent new secure tunnel between the wireless device and the server after the first secure tunnel has been torn down and upon determining the shared secret exists by using the shared secret to mutually derive a tunnel key using symmetric cryptography based on the shared secret;

wherein the wireless device is configured to mutually authenticate with the server employing the subsequent new secure tunnel; and

wherein the wireless device is configured to derive keying material that binds the subsequent new secure tunnel with all conversations inside the subsequent new secure tunnel.

26. A wireless device according to claim 24, wherein the wireless device is further configured to establish a session key seed for deriving a master session key used for mutually authenticating the wireless device employing the secure tunnel.

27. A method according to claim 1, further comprising establishing a plurality of subsequent new secure tunnels between the peer and server using the shared secret.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.